UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,862	02/25/2004	Sergey Shokhor	08204/0200873-US0	3678

38878 7590 05/06/2009

F5 Networks, Inc.
c/o DARBY & DARBY P.C.
P.O. BOX 770
Church Street Station
NEW YORK, NY 10008-0770

EXAMINER	
KEEHN, RICHARD G	

ART UNIT	PAPER NUMBER
2456	

MAIL DATE	DELIVERY MODE
05/06/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/786,862	SHOKHOR ET AL.	
	Examiner	Art Unit	
	Richard G. Keehn	2456	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 April 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-33 have been examined and are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/1/2009 has been entered.

Response to Arguments

2. Applicant's arguments, see page 10, filed 4/1/2009, with respect to the rejection of Claims 1, 22, 28 and 31 under 35 U.S.C. 112 have been fully considered and are persuasive. The previous rejection of Claims 1, 22, 28 and 31 has been withdrawn. However new 35 U.S.C. 112 rejections exist (see below).

3. Applicant's arguments with respect to the prior art rejection of claims 1-33 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

4. Claim 17 is objected to because of the following informalities: Improper tense of the word "comprise." Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claim 1 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The amended limitation “including determining whether client security software beyond a virtual sandbox is active on the client device” introduces the concept of determining “beyond.” There is no support in the specification, drawings or originally submitted claims for "determining…beyond a virtual sandbox."

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1, 2, 8, 22, 23, 25-27 and 31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Regarding claims 1 and 31, the phrase "arranged to" renders the claims indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

10. Regarding claims 2, 8, 22, 23 and 25-27, the phrase "configured to" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Specification

11. The amendment filed 4/1/2009 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: The amended limitation "including determining whether client security software beyond a virtual sandbox is active on the client device" introduces the concept of determining "beyond." There is no support in the specification for "beyond."

Applicant is required to cancel the new matter in the reply to this Office Action.

Drawings

12. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the virtual sandbox, kiosk and hacker tool must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate

prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

14. Claim 32 is rejected under 35 U.S.C. 102(e) as being anticipated by US 7,308,703 B2 (Wright et al.).

As to Claim 32, Wright et al. anticipate a method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device (Wright et al. disclose reception of client request – Column 15, lines 62-63);

determining a level of security software enabled on the client device (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64)

including what antivirus software is active on the client device (Wright et al. disclose policy based on anti-virus software status - Column 18. lines 35-39)

and whether a hacker tool is enabled on the client device (Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN);

applying a dynamic policy to the access based, in part, on the determined level of security software enabled (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64); and

applying a restriction to the access for the requested resource based on the applied dynamic policy (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64).

Claim Rejections - 35 USC § 103

15. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

16. Claims 1, 2, 4-11, 13-18 and 20-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 7,308,703 B2 (Wright et al.), and further in view of US 7,430,524 B2 (Shah et al.).

As to Claims 1, 10, 22, 28 and 31, Wright et al. disclose an apparatus, method, a network appliance and a computer readable storage medium that includes data and instructions, wherein the execution of the instructions on a computing device provides, and an apparatus, respectively, for managing access to a resource over a network, comprising:

a receiver arranged to receive a request for access to the resource from a client device (Wright et al. disclose reception of client request – Column 15, lines 62-63); and

a policy manager, coupled to the receiver, that is arranged to perform actions, including (Wright et al. disclose the policy module – Column 15, lines 40-42):

including determining whether client security software beyond a virtual sandbox is active on the client device (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64);

the configuration of the client device based on the inspection (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64);

applying a dynamic policy for the access based, in part, on the received configuration (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64); and

applying a restriction to the access for the requested resource based on the applied dynamic policy (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64);

and whether a hacker tool is enabled on the client device (**CLAIM 31 Only**) (Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN).

Wright et al. do not disclose downloading a component onto the client device, wherein the downloaded component inspects the client device to detect a configuration of the client device and receiving from the downloaded component, but Shah et al. disclose

downloading a component onto the client device, wherein the downloaded component inspects the client device to detect a configuration of the client device (Shah et al. – Column 76, lines 9-25 disclose downloading an agent onto a client

device to inspect the client device to determine the client device's configuration, and reporting said configuration back to the server that sent the agent); and

receiving from the downloaded component (Shah et al. – Column 76, lines 9-25 disclose downloading an agent onto a client device to inspect the client device to determine the client device's configuration, and reporting said configuration back to the server that sent the agent).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine sending an agent to determine a client's configuration and reporting back to the sender taught by Shah et al. with determining the client configuration taught by Wright et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to determine information regarding a plurality of client devices for system modeling (Shah et al. – Column 76, lines 40-51).

As to Claim 2, the combination of Wright et al. and Shah et al. discloses the apparatus of claim 1, wherein determining the configuration of the client device further comprises:

if the client device is configured to not download the component, then receiving the configuration of the client device through a browser residing on the client device (Shah et al. disclose the server capable of determining client's configuration via a plug and play interface which those of ordinary skill in the art would know to include plug and

play browsers, as an alternative to the downloadable component determining the configuration and sending it back to the server – Column 76, lines 15-22).

The motivation and obviousness arguments are the same as in Claim 1.

As to Claim 4, the combination of Wright et al. and Shah et al. discloses the apparatus of claim 1, wherein determining the configuration of the client device further comprises

determining information associated with the connection between the client device and the resource (Wright et al. disclose determining information associated with the communication session between the mobile device and another computer – Column 3, lines 4-8).

As to Claim 5, the combination of Wright et al. and Shah et al. discloses the apparatus of claim 1, wherein inspecting the client device to detect a configuration further comprises

detecting if security software is installed on the client device and if security software is installed, inspecting the security software to detect if the security software is active or disabled (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64).

As to Claim 6, the combination of Wright et al. and Shah et al. discloses the apparatus of claim 1, wherein applying the restriction further comprises

employing a virtual sandbox that is configured based on the applied dynamic policy (Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN, the VPN being a virtual sandbox).

As to Claim 7, the combination of Wright et al. and Shah et al. discloses the apparatus of claim 1,

wherein the restriction includes at least one downloadable component (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64).

As to Claim 8, the combination of Wright et al. and Shah et al. discloses the apparatus of claim 1,

wherein the restriction is configured to intercept a communication between the client device and the apparatus (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67).

As to Claim 9, the combination of Wright et al. and Shah et al. discloses the apparatus of claim 1, wherein applying the restriction further comprises

performing at least one of intercepting a system command, inhibiting a file save, inhibiting a file print, restricting launching of a predetermined application, and redirecting access to a file (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67).

As to Claim 11, the combination of Wright et al. and Shah et al. discloses the method of claim 10, further comprising

in response to receiving the request for access to the resource, transmitting a downloadable component to the client device (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64).

As to Claim 13, the combination of Wright et al. and Shah et al. discloses the method of claim 10, wherein receiving the configuration further comprises:

receiving information indicating at least one of one level of trust associated with the client device, a type of encryption enabled on the client device, a type of antivirus enabled on the client device, a security feature enabled on the client device, a browser type, an operating system configuration, a security certificate, and if a hacker tool is enabled on the client device (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64; Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN).

As to Claim 14, the combination of Wright et al. and Shah et al. discloses the method of claim 10, wherein receiving the configuration further comprises:

receiving information indicating a level of trust of the client device (Wright et al disclose the trust level determination – Column 18, lines 19-23).

As to Claim 15, the combination of Wright et al. and Shah et al. discloses the method of claim 10, wherein receiving the configuration further comprises:

receiving information indicating a characteristic of an enabled security application enabled (Wright et al disclose the trust level determination – Column 18, lines 19-23).

As to Claim 16, the combination of Wright et al. and Shah et al. discloses the method of claim 10, wherein applying the restriction further comprises

downloading a component to the client device (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64).

As to Claim 17, the combination of Wright et al. and Shah et al. discloses the method of claim 10, wherein applying the restriction further comprise [*sic*]

configuring a virtual sandbox to intercept a communication between the client device and the resource (Wright et al. discloses the interception of files as a restriction –

Column 7, lines 59-67; Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN, the VPN being a virtual sandbox).

As to Claim 18, the combination of Wright et al. and Shah et al. discloses the method of claim 17, wherein intercepting the communication further comprises

blocking a download of at least one file to the client device (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67).

As to Claim 20, the combination of Wright et al. and Shah et al. discloses the method of claim 10, wherein applying the dynamic policy further comprises

determining at least one of a connector, and an adaptor to enable the access to the resource (Wright et al. disclose the determination of network adapter - Column 7, lines 26-37).

As to Claim 21, the combination of Wright et al. and Shah et al. discloses the method of claim 10, wherein applying the dynamic policy further comprises

restricting the access to the resource (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67).

As to Claim 23, the combination of Wright et al. and Shah et al. discloses the network appliance of claim 22, wherein the processor is configured to perform further actions, comprising:

in response to receiving the request for access to the resource, receiving additional information about the configuration of the client device through a query with a browser residing on the client device (Shah et al. – Column 76, lines 15-22 disclose the server capable of determining client's configuration via a plug and play interface which those of ordinary skill in the art would know to include plug and play browsers, as an alternative to the downloadable component determining the configuration and sending it back to the server).

The motivation and obviousness arguments are the same as in Claim 1.

As to Claim 24, the combination of Wright et al. and Shah et al. discloses the network appliance of claim 22, wherein applying the restriction further comprises

employing a virtual sandbox that is configured based on the applied dynamic policy (Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN, the VPN being a virtual sandbox).

As to Claim 25, the combination of Wright et al. and Shah et al. discloses the network appliance of claim 23, wherein determining the configuration of the client device further comprises:

if the client device is not configured to receive a downloadable component, receiving information about the configuration of the client device through a browser application residing within the client device (Shah et al. disclose the server capable of determining client's configuration via a plug and play interface which those of ordinary

skill in the art would know to include plug and play browsers, as an alternative to the downloadable component determining the configuration and sending it back to the server – Column 76, lines 15-22).

The motivation and obviousness arguments are the same as in Claim 1.

As to Claim 26, the combination of Wright et al. and Shah et al. discloses the network appliance of claim 22, wherein applying the dynamic policy further comprises:

if the client device is configured to restricting a download of a component, restricting access to the resource (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64).

As to Claim 27, the combination of Wright et al. and Shah et al. discloses the network appliance of claim 22, wherein applying the restriction further comprises:

if the client device is configured to restrict a download of a component, intercepting a communication between the client device and the requested resource to perform at least one of preventing an access to file, and restricting an action (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67).

As to Claim 29, the combination of Wright et al. and Shah et al. discloses the computer readable storage medium of claim 28, wherein applying the restriction further comprises

configuring a Virtual sandbox to intercept a communication between the client device and the resource (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67; Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN, the VPN being a virtual sandbox).

As to Claim 30, the combination of Wright et al. and Shah et al. discloses the computer readable storage medium of claim 28, wherein applying the restriction further comprises

blocking a download of at least one file to the client device (Wright et al. discloses the interception of files as a restriction – Column 7, lines 59-67).

17. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Wright et al. and Shah et al. as applied to claim 10 above, and further in view of US 7,200,272 B2 (Ishikawa).

As to Claim 19, the combination of Wright et al. and Shah et al. discloses the method of claim 10.

The combination of Wright et al. and Shah et al. does not disclose if the access to the resource is terminated, performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command, but Ishikawa discloses, wherein applying the restriction further comprises:

if the access to the resource is terminated, performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command (Ishikawa – Column 5, lines 2-12 disclose the client's cache manager deleting the user's cache as part of a cleanup).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine performing cleanup on the client device including at least one of deleting a cached file, deleting a temporary file, and enabling a disabled system command taught by Ishikawa, with applying a restriction to the access for the requested resource based on the applied dynamic policy taught by the combination of Wright et al. and Shah et al.

One of ordinary skill in the art at the time the invention was made would have been motivated to avoid system resources from sitting at their maximum limit, thus freeing up resources for other applications to use (Ishikawa - Column 5, lines 8-12).

18. Claims 3 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 7,308,703 B2 (Wright et al.), and further in view of US 2002/0111852 A1 (Levine).

As to Claim 3, the combination of Wright et al. and Shah et al. discloses the apparatus of claim 1.

The combination of Wright et al. and Shah et al. does not disclose wherein the received configuration indicates whether the client device is operating as a kiosk, but Levine discloses

wherein the received configuration indicates whether the client device is operating as a kiosk (Levine – Page 2, ¶ [0022] discloses determining the type of client device and whether it's a cell phone, kiosk, PDA, laptop, desk computer, terminal or any other access device).

The motivation and obviousness arguments are similar to that of Claim 33.

As to Claim 12, the combination of Wright et al. and Shah et al. discloses the method of claim 10, wherein receiving the configuration further comprises.

The combination of Wright et al. and Shah et al. does not disclose receiving information indicating whether the client device is a laptop, personal computer, kiosk, or a mobile device, but Levine discloses

receiving information indicating whether the client device is a laptop, personal computer, kiosk, or a mobile device (Levine – Page 2, ¶ [0022] discloses determining the type of client device and whether it's a cell phone, kiosk, PDA, laptop, desk computer, terminal or any other access device).

The motivation and obviousness arguments are similar to that of Claim 33.

19. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 7,308,703 B2 (Wright et al.), and further in view of US 2002/0111852 A1 (Levine).

As to Claim 33, Wright et al. disclose a method for managing access to a resource over a network, comprising:

receiving a request for access to the resource from a client device (Wright et al. disclose reception of client request – Column 15, lines 62-63);

determining whether client computing security software is active on the client device or whether a hacker tool is enabled on the client device (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64; Wright et al. Column 20, lines 35-42 disclose that the security software can be a hacker tool VPN); and

applying a restriction to the access for the requested resource based on the determined configuration of the client device (Wright et al. disclose determining a client's security software status as active or inactive and basing restrictions to client access based on the client's security status – Column 2, lines 17-64).

Wright et al. do not explicitly disclose determining if the client device is configured as a kiosk or a mobile device, but Levine discloses

determining if the client device is configured as a kiosk or a mobile device (Levine – Page 2, ¶ [0022] discloses determining the type of client device and whether it's a cell phone, kiosk, PDA, laptop, desk computer, terminal or any other access device).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine determining if the client device is configured as a kiosk or a mobile device taught by Levine, with determining client configuration taught by Wright et al., in order to personalize content delivery (Levine – Page 2, ¶ [0015]).

Examiner Notes

20. Page 5, line 23 of the specification recites the use of IPSec VPN. Similar distinguishing features can be found on Pages 6 and 12 of the specification. These features are disclosed, but not included in the claim language. Including them in independent form would overcome the references cited in this prior art rejection.

Conclusion

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. These include:

US 7,322,044 B2	Systems and methods for automated network policy exception detection and correction
US 6,990,591 B1	Method and system for remotely configuring and monitoring a communication device
US 6,925,495 B2	Method and system for delivering and monitoring an on-demand playlist over a network using a template
US 7,313,822 B2	Application-layer security method and system
US 6,502,131 B1	Directory enabled policy management tool for intelligent traffic management
US 7,313,618 B2	Network architecture using firewalls
US 6,917,980 B1	Method and apparatus for dynamic modification of

	internet firewalls using variably-weighted text rules
US 5,319,562 A	System and method for purchase and application of postage using personal computer
US 6,981,257 B2	System, method and apparatus to allow communication between CICS and non-CICS software applications
US 7,257,623 B2	Method and apparatus for ensuring an allowable client configuration for an application
US 7,237,263 B1	Remote management of properties, such as properties for establishing a virtual private network
US 6,944,761 B2	Log-on service providing credential level change without loss of session continuity
US 7,328,453 B2	Systems and methods for the prevention of unauthorized use and manipulation of digital content
US 7,260,224 B1	Automated secure key transfer
US 7,260,388 B1	Communication device qualification for broadband wireless service
US 7,269,847 B2	Firewall providing enhanced network security and user transparency
US 7,007,025 B1	Method and system for maintaining secure data input and output
US 7,181,731 B2	Method, system, and structure for distributing and

	executing software and data on different network and computer devices, platforms, and environments
US 6,684,253 B1	Secure segregation of data of two or more domains or trust realms transmitted through a common data channel
US 7,337,174 B1	Logic table abstraction layer for accessing configuration information
US 7,272,855 B1	Unified monitoring and detection of intrusion attacks in an electronic system
US 7,139,811 B2	Double-proxy remote data access system
US 6,687,831 B1	Method and apparatus for multiple security service enablement in a data processing system
US 6,993,663 B1	Input buffer overrun checking and prevention

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Richard G. Keehn whose telephone number is 571-270-5007. The examiner can normally be reached on Monday through Thursday, 9:00am - 8:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

RGK

/Yasin M Barqadle/
Primary Examiner, Art Unit 2456